Ahmed Tamer Samir

ahmedtamersamirml@gmail.com
01112209447
Maadi-Cairo
linkedin.com/in/ahmed-tamer-b8699b282
github.com/AhmedTamergithub

Education

2020 – 2025

B.Sc. Electronics and Electrical Communications Engineering
Cairo University

Cumulative Grade: Very Good (80%)
Fourth Year Grade: Excellent (89%)

Professional Experience

2025/07 – 2025/09

AI Full-Time Internship
TechnoWelle GmbH
Contributed to the development of an Agentic AI system for automating the Hardware-in-the-Loop (HIL) testing process in automotive embedded systems. The system consisted of 7 agents that streamlined the entire workflow: from generating comprehensive test plans, to producing code-agnostic test cases across multiple HIL languages, to executing these tests on real hardware with automated issue reporting. It supported two major HIL testbenches: Vector Informatik VT System and Technowelle's proprietary HIL. This project strengthened my expertise in AI agents, Large Language Models (LLMs), Retrieval-Augmented Generation (RAG), modern agent protocols (MCP, A2A), LLM fine-tuning, and advanced prompt engineering strategies.

2024/10 – 2025/06

Graduation Project
Sponsored by Si-Vision
Designed and evaluated deep learning systems under adversarial attack scenarios to study model vulnerabilities and robustness in both computer vision (CV) and natural language processing (NLP), including large language models (LLMs).
Key Contributions:

- **Model Development:**

Built and fine-tuned models like Image Classification EfficientNet Model (CV) and Sentiment Analysis / LLMs (NLP).

- **Adversarial Attacks:**

CV Attacks: FGSM, PGD, MI-FGSM, SIMBA, ElasticNet, JSMA
NLP Attacks: UAP, HotFlip, DeepWordBug
LLM Attacks: Jailbreak Attacks, Prompt Injection

- **Defensive Techniques:**

CV Defenses: Adversarial Training, Noise Fusion, Gradient Masking
LLM Defenses: Input/Output Filtering, Rewindable Autoregressive Inference (RAIN)
,**Most Highlighted Contribution in LLMs** : Implementing an Input Filtering Defense from scratch by fine-tuning DistilBert LLM using LoRA technique to distinguish between jailbreak & safe prompts achieving a reduction in Attack success rate from 87% to 0%

2024/07 – 2024/09

SW Engineering intern
LXT AI
Full Stack Developer – Worked on backend and frontend teams.
Final Project: Full-stack To-Do List app with React (frontend), FastAPI (Python backend), and PostgreSQL (database).

Projects

- **Agentic Arabic Prompt Engineer**

Built an autonomous agent with LangChain that refines Arabic prompts via multi-step reasoning, self-evaluation, and feedback optimization.

- **Arabic Q/A RAG System**
  Building a RAG system using an Arabic book as the knowledge base. The book was split into short paragraphs, embedded with a multilingual model, and indexed with FAISS. For each Arabic query, relevant text is retrieved and passed to an LLM to generate an answer. We also compared this with LLM-only answers.

- **Implementation of EfficientNet Model**
  Implementing EfficientNet from scratch that is used for Image Classification using Pytorch Framework and training it over various Datasets like: FashionMnist and Cifar10 and then applying on it Adversarial attacks to test Model robustness like FGSM,PGD,Simba and ElasticNet

- **Implementation a Sentiment Analysis NLP model**
  Implementing Sentiment Analysis NLP Model from Scratch and training it on datasets like IMDB reviews and YelpReviews and then attacking the models with textual based NLP specified attacks like Character &word-level attacks like Deepwordbug,UAP and DeepFool to test model robustness to attacks and applying the concept of Adversarial attacks.

- **DoorLocker Security System**
  Developing a system to unlock a door using a password. Drivers: GPIO, Keypad, LCD, Timer, UART, I2C, EEPROM, Buzzer and DC-Motor - Microcontroller: ATmega32

- **Implementing STM32 BlueBill (CortexM3) Drivers**
  Implemented STM drivers on BluePill (Cortex-M3) board, enhancing my skills in ARM architecture.

- **Implementing full MCAL and HAL Drivers for AVR ATmega32 efficiently for various applications**

- **Design of SPI slave wrapper with a single port Asynchronous RAM using Verilog HDL**

- **Design of Spartan6-DSP48A1 using Verilog HDL**

- **Design of synchronous FIFO using Verilog HDL**

- **Development of a complete top-level UVM environment for SPI-Slave connected to Dual-port RAM and ALSU unit**

- **Design of an Arithmetic Logic Shift Unit (ALSU) using Verilog and implemented on FPGA**

Skills

Machine Learning Concepts
Supervised learning, Regression, Classification, Neural networks, Python ML libraries

Natural Language Processing
Embeddings, Sentiment Analysis, Text Classification, Tokenization, NER

Generative AI
LLMs, AI agents, RAG Pipelines, LLM fine-tuning (PEFT – LoRA), AI Safety & Alignment

Modern AI Agent Protocols
MCP,A2A

Programming Languages
C,C++,Python

Hardware Description Languages:
Verilog and System-Verilog

Digital IC Design & Verification Basics
RTL Design, Functional Verification, Testbench Development, UVM Basics,Assertions,STA,Synthesis

Web Frameworks
FastAPI,React

Databases and Query Languages
SQL,PostgreSQL,SQLite

Computer Vision
Image Classification,Object Detection

Deep Learning FrameWorks
TensorFlow,PyTorch,Keras

AI Agents Frameworks
Google-ADK,LangChain,smolagents

LLM APIs & Frameworks
OpenAI API (GPT models),
Hugging Face Transformers,
Ollama (local LLM serving)

Data Structures and OOP Concepts

Scripting Languages
TCL and Bash Shell

Microcontroller Interfacing
AVR,ARM

Frontend Web Development Languages
HTML,CSS,JavaScript

Tools
Proteus,Docker,Postman,Questasim,Vivado,Matlab, Eclipse IDE, STM32CubeIDE